

Release Notes for Cisco Identity Services Engine, Release 2.4

First Published: 2018-04-30

Last Modified: 2018-05-03



Note Come to the Content Hub at content.cisco.com, where, using the Faceted Search feature, you can accurately zoom in on the content you want; create customized PDF books on the fly for ready reference; and can do so much more...

So, what are you waiting for? Click content.cisco.com now!

And, if you are already experiencing the Content Hub, we'd like to hear from you!

Click the **Feedback** icon on the page and let your thoughts flow!

Introduction

Cisco Identity Services Engine (ISE) is a security policy management platform that provides secure access to network resources. Cisco ISE functions as a policy decision point and enables enterprises to ensure compliance, enhance infrastructure security, and streamline service operations. Cisco ISE allows enterprises to gather real-time contextual information from networks, users, and devices. An administrator can then use this information to make proactive governance decisions by creating access control policies for the various network elements, including access switches, wireless LAN controllers (WLCs), Virtual Private Network (VPN) gateways, and data center switches. Cisco ISE acts as the policy manager in the Cisco TrustSec solution and supports TrustSec software-defined segmentation.

The Cisco ISE platform is a comprehensive, next-generation, contextually-based access-control solution. It offers authenticated network access, profiling, posture, Bring Your Own Device (BYOD) onboarding (native supplicant and certificate provisioning), guest management, device administration (TACACS+), and security group access services along with monitoring, reporting, and troubleshooting capabilities on a single physical or virtual appliance.

Cisco ISE is available on two physical appliances with different performance characterizations, and also as software that can be run on a virtual machine. You can add more appliances to a deployment for performance, scale, and resiliency.

Cisco ISE has a scalable architecture that supports standalone and distributed deployments, but with centralized configuration and management. It also allows for configuration and management of distinct personas and services, thereby giving you the ability to create and apply services where needed in a network, but still operate the Cisco ISE deployment as a complete and coordinated system.

For more information about the features that are supported in Cisco ISE 2.4, see [Cisco Identity Services Engine Administrator Guide, Release 2.4](#).

System Requirements

- [Supported Hardware](#)
- [Supported Virtual Environments](#)
- [Supported Browsers](#)
- [Support for Microsoft Active Directory](#)
- [Supported Antivirus and Antimalware Products](#)



Note For more details on Cisco ISE hardware platforms and installation, see the Cisco Identity Services Engine Hardware Installation Guide.

Supported Hardware

Cisco ISE, Release 2.4, is shipped on the following platforms. After installation, you can configure Cisco ISE with specified component personas (Administration, Policy Service, Monitoring, and pxGrid) on the platforms that are listed in the following table.

Table 1: Supported Hardware and Personas

Hardware Platform	Persona	Configuration
Cisco SNS-3515-K9 (small)	Any	See the Cisco Identity Services Engine Hardware Installation Guide for appliance hardware specifications.
Cisco SNS-3595-K9 (large)		
Cisco ISE-VM-K9 (VMware, Linux KVM, Microsoft Hyper-V)		<ul style="list-style-type: none"> • For CPU and memory recommendations, see the “VMware Appliance Sizing Recommendations” section in the Cisco Identity Services Engine Hardware Installation Guide, Release 2.4. • For hard disk size recommendations, see the “Disk Space Requirements” section in the Cisco Identity Services Engine Hardware Installation Guide, Release 2.4. • NIC—1-GB NIC interface required. You can install up to 6 NICs. • Supported virtual machine versions include: <ul style="list-style-type: none"> • ESXi 5.x (5.1 U2 and later support RHEL 7), 6.x • Microsoft Hyper-V on Microsoft Windows Server 2012 R2 and later • KVM on: <ul style="list-style-type: none"> • RHEL 7.3 • Ubuntu 14.04 LTS <p>Note If you are installing or upgrading Cisco ISE on an ESXi 5.x server, to support RHEL 7 as the Guest OS, update the VMware hardware version to 9 or later. RHEL 7 is supported with VMware hardware Version 9 and later.</p>

**Note**

- Cisco SNS 3400 series appliances are not supported with Cisco ISE, Release 2.4 and later.
- Memory allocation of less than 16 GB is not supported for any VM appliance configuration. In the event of a Cisco ISE behavior issue, all users will be required to change allocated memory to at least 16 GB before opening a case with the Cisco Technical Assistance Center.
- Legacy ACS and NAC appliances (including the Cisco ISE 3300 Series) are not supported with Cisco ISE, Release 2.0 and later.

FIPS Mode Support

Cisco ISE uses embedded Federal Information Processing Standard (FIPS) 140-2-validated cryptographic module, Cisco FIPS Object Module Version 6.0 (Certificate #2505). For details about the FIPS compliance claims, see the [Global Government Certifications](#).

Supported Virtual Environments

Cisco ISE supports the following virtual environment platforms:

- ESXi 5.x (5.1 U2 and later support RHEL 7), 6.x
- Microsoft Hyper-V on Microsoft Windows Server 2012 R2 and later
- KVM on:
 - RHEL 7.3
 - Ubuntu 14.04 LTS

**Note**

For the installations on Ubuntu, the user must validate the product name reflecting in the output in dmidecode.

Dmidecode utility reads from SMBIOS. If the "system-product" string does not contain "KVM", the readUDI will be unable to determine the type of virtualization and 'validate_platform_info()' in ks.cfg will fail, displaying the following error message.

ERROR: UNSUPPORTED HARDWARE DETECTED!

Update the applicable product name (in a string format) on the VM BIOS from the list below:

```
#define KVM_DMI_PRODNAME "KVM"
#define HyperVstr "Virtual Machine"
#define VMstr "VMware"
#define VMstr "VMware"
```



Note If you are installing or upgrading Cisco ISE on an ESXi 5.x server to support RHEL 7 as the Guest OS, update the VMware hardware version to 9 or later. RHEL 7 is supported with VMware hardware version 9 and later.

Supported Browsers

Supported browsers for the Admin portal include:

- Mozilla Firefox 61 and earlier versions
- Google Chrome 67 and earlier versions



Note If you use Chrome 65.0.3325.189, you may be unable to view guest account details in the print preview section.

- Microsoft Internet Explorer 10.x and 11.x

If you are using Internet Explorer 10.x, enable TLS 1.1 and TLS 1.2, and disable SSL 3.0 and TLS 1.0 (Internet Options > Advanced).

Support for Microsoft Active Directory

Cisco ISE, Release 2.4, works with Microsoft Active Directory servers 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2, and 2016 at all functional levels.



Note Microsoft has ended support for Windows Server 2003 and 2003 R2. We recommend that you upgrade Windows Server to a supported version.

Microsoft Active Directory Version 2000 or its functional level is not supported by Cisco ISE.

Cisco ISE 2.4 supports multidomain forest integration with Active Directory infrastructures to support authentication and attribute collection across large enterprise networks. Cisco ISE 2.4 supports up to 50 domain join points.

Improved User Identification

ISE has improved its ability to identify Active Directory users when a username is not unique. Duplicate usernames are common when using short usernames in a multi-domain AD environment. You can identify users by SAM, CN, or both. ISE uses the attributes that you make available to uniquely identify a user.

To configure which attributes ISE uses to resolve user identity, edit the registry on the server running Active Directory, and update the value of

```
REGISTRY.Services\lsass\Parameters\Providers\ActiveDirectory\IdentityLookupField
```

- SAM - to use only the SAM in the query (the default).

- CN - to use only CN in the query.
- CNSAM - to use CN and SAM in the query.

Supported Antivirus and Antimalware Products

For more information on the products supported by the ISE posture agent, see the Cisco AnyConnect ISE Posture Support Charts at:
<https://www.cisco.com/c/en/us/support/security/identity-services-engine/products-device-support-tables-list.html>

What is New in Cisco ISE, Release 2.4

Cisco ISE Can Pull IoT Device Context and Session Data from Cisco IND

Cisco ISE can profile and display the status of devices attached to a Cisco Industrial Network Director (IND). Cisco Platform Exchange Grid (pxGrid) is used to communicate the endpoint (Internet of Things [IoT]) data between Cisco ISE and Cisco IND. pxGrid is used to receive the context from Cisco IND and query Cisco IND to update endpoint type.

Business Outcome

Effective network monitoring and full visibility and control of industrial networks offer:

- Full visibility and control of automation endpoints, such as controllers, IO devices, and human machine interfaces (HMIs).
- Lowered asset management cost and improved operator productivity with Cisco IND and Cisco ISE integration.

Control Permissions for pxGrid Clients

You can create pxGrid authorization rules for controlling the permissions for the pxGrid clients (under Administration > pxGrid Services > Permissions).

Use these rules to control the services that are provided to the clients. You can create different types of groups and map the services that are provided to clients to these groups. Use the Manage Groups option in the Permissions window to add new groups. You can view the predefined authorization rules that use predefined groups (such as EPS, ANC) on the Permissions window. You can update only the Operations field in the predefined rules.

Business Outcome

Better pxGrid backward compatibility:

- Ability to control authorizations for different pxGrid services.
- Easier to group pxGrid clients with similar permissions.

Customizable SSH Ciphers and Encryption Algorithms

You can use the `service ssh encryption-algorithm` and `service ssh encryption-mode` global configuration commands in Cisco ISE 2.4 to harden the ISE SSH server and specify the cipher suite to be used. You can use AES-CTR and/or AES-CBC ciphers.

Cisco ISE 2.3 and earlier releases allowed only AES-CBC ciphers (due to Common Criteria Protection Profiles for Access Control Devices and Systems). Cisco ISE 2.4 allows you to use both AES-CTR and AES-CBC ciphers.

Business Outcome

- Improved security for SSH access.
- Allows you to choose the encryption algorithms.
- Allows you to choose the ciphers to be used to harden secure access.

Endpoint API Enhancements for MDM Attributes

Mobile Device Management (MDM) attributes are made available through the endpoints API to enable additional synchronization capability between Cisco ISE and a third-party MDM server.

Business Outcome

Helps customers to better integrate third party systems with ISE and provide better user experience for end users using mobile devices that are managed by an MDM server.

IPv6 Support for RADIUS

IPv6 addresses are now supported for RADIUS configurations. The IP Address field in the Administration > Network Resources > Network Devices page and the Host IP field in the Administration > Network Resources > External RADIUS Server page now support both IPv4 and IPv6 addresses for RADIUS configurations.

Business Outcome

Additional support for IPv6 addressing:

- Allows you to migrate your network to IPv6-based networks. You can migrate to IPv6 addressing if you have fragmented networks or have exhausted IPv4 addresses.
- Facilitates more efficient routing, packet processing, security, and simplified network configuration.

Large Virtual Machine for Monitoring Persona

Cisco ISE introduces a large VM for Monitoring nodes.

This form factor is available only as a VM in Release 2.4 and above, and requires a large VM license.

Business Outcome

Deploying Monitoring persona on a large VM offers the following advantages:

- Up to three times the volume of data previously supported.
- Improved performance in terms of faster response to live log queries and report completion.

Posture Enhancements

- **Grace Period for Noncompliant Devices**—Cisco ISE provides an option to configure grace time for devices that become noncompliant. Cisco ISE caches the results of posture assessment for a configurable amount of time. If a device is found to be noncompliant, Cisco ISE looks for the previously known good state in its cache and provides grace time for the device, during which the device is granted access to the network. You can configure the grace time period in minutes, hours, or days (up to a maximum of 30 days). The Posture Assessment by Endpoint report is updated and displays a Grace Compliant status for an endpoint that is currently not compliant, but is under the grace period.
- **Posture Rescan**—AnyConnect users can now manually restart posture at any time.
- **AnyConnect Stealth Mode Notifications**—Several new failure notifications are added for AnyConnect stealth mode deployment to help users identify issues with their VPN connection.
- **Disabling UAC Prompt on Windows**—You can choose to disable the User Access Control (UAC) prompts on Windows endpoints from the AnyConnect posture profile.



Note By default, this value is set to No while configuring the AnyConnect Profile. When you change it to Yes, the UAC prompts are disabled and the Windows users no longer receive these prompts. If you want to enable the UAC prompt again, you should change this setting to No in the AnyConnect Profile. This setting takes effect only when the Windows endpoint is restarted.

- **New URL for Downloading Client Provisioning and Posture Updates**—The client provisioning and posture feed URL has changed. The new URL for Posture Updates is <https://www.cisco.com/web/secure/spa/posture-update.xml> and for Client Provisioning is <https://www.cisco.com/web/secure/spa/provisioning-update.xml>
- **File Condition Enhancements**—A new operator, within, is introduced under File Condition to check for the changes in a file within a certain period of time.
- **Certificate Attributes in Client Provisioning and Posture Policies**—Certificate attributes are now available in the client provisioning and posture policy pages.
- The following option has been newly added under the Location field in the Policy > Policy Elements > Conditions > Posture > Disk Encryption Condition window:
 - **All Internal Drives**—To check the internal drives. Includes all hard disks that are mounted and encrypted, and all internal partitions. Excludes read only drives, system recovery disk/partition, boot partition, network partitions, and the different physical disk drives that are external to the endpoint (including but not limited to disk drives connected via USB and Thunderbolt). Encryption software products that are validated include:

- Bit-locker-6.x/10.x
- Checkpoint 80.x on Windows 7



Note "All Internal Drives" option is supported from AnyConnect Version 4.6.01098 onwards.

Business Outcome

Improved security alerts and enforcement:

- Provides admin users with more flexible options for educating end users about posture condition failures including grace-period-specific messaging scenarios.
- Helps effective management of some posture checks and remediations that require additional privileges and prompts the user for such privileges.

Profiler Enhancements

- Added 630 new profile policies from vendors, including AudioCode, BlackBerry, Brother, Hewlett Packard, Lexmark, NetApp, Samsung, and Xerox.
- Added additional conditions to 185 profile policies to support additional probes. For example, DHCP conditions are added to Xerox devices such that customers who do not want to profile Xerox devices based on SNMP, can profile Xerox devices using DHCP.
- Reorganized profiles into families for better identification of new devices. For example, HP-LaserJet-4350 was previously profiled directly under HP-Device. It is now profiled under HP-LaserJet, which in turn is profiled under HP-Device. When Hewlett Packard introduces a new Hewlett Packard LaserJet printer model, Cisco ISE will classify the new model as HP-LaserJet, and not as HP-Device until a new profile policy for that exact LaserJet printer model is added.

Business Outcome

Effective classification of devices:

- Helps you gain visibility of previously unknown devices, such as Xerox printers or Vista link printers with improved profiler efficacy.

Support for Sending Separate SNMP CoA Packets

You can check the **Send SNMP CoA Separate Request** check box in the **Administration > Network Resources > Network Device Profiles > Change of Authorization (CoA)** window to send the SNMP CoA packets to the NAD as two packets.

Business Outcome

Increased compatibility with devices:

- Provides support for older Cisco and third-party NADs that mandate the sending of SNMP CoA packets as two packets (for the shutdown and no shutdown interface configuration commands).

Support for Two Shared Secrets Per IP for RADIUS NAD Clients

You can specify two shared secrets (keys) to be used by the network device and Cisco ISE. You can configure the shared secrets in the RADIUS authentication settings section for a NAD in the Administration > Network Resources > Network Devices page in Cisco ISE.

Business Outcome

Replace Shared Secrets on network devices:

- Enables you to replace shared secrets on network devices independently and allows ISE to support both old and new shared secrets until the shared secret is replaced on the network device. Changing a RADIUS secret is now simplified and allows you to enter a new shared secret even before updating the network device.

TrustSec Enhancements

You can select the ISE node from which the configuration changes must be sent to the network device while adding the network device (under **Advanced TrustSec Settings** section). You can select the PAN or PSN node. If the PSN node that you selected is down, the configuration changes are sent to this device using the PAN.

While deploying the IP SGT static mappings, you can select the devices or the device groups to which the selected mappings must be deployed. You can select all the devices if necessary. You can use the filter option to search for the devices that you want. If you do not select any device, the selected mappings are deployed on all TrustSec devices.

You can use the **Check Status** option to check if different SGTs are assigned to the same IP address for a specific device. You can use this option to find the devices that have conflicting mappings, IP address that is mapped to multiple SGTs, and the SGTs that are assigned to the same IP address. This option can be used even if device groups, FQDN, hostname, or IPv6 addresses are used in the deployment. You must remove the conflicting mappings or modify the scope of deployment before deploying these mappings.

Verify TrustSec Deployment option on the **General TrustSec Settings** page helps you to verify whether the latest TrustSec policies are deployed on all the network devices. Alarms are displayed in the **Alarms** dashlet (under **Work Centers > TrustSec > Dashboard**), if there are any discrepancies between the policies that are configured on Cisco ISE and the network device. The following alarms are displayed in the TrustSec dashboard:

- An alarm with an Info icon is displayed whenever the verification process is started or completed.
- An alarm with an Info icon is displayed if the verification process is cancelled due to a new deployment request.
- If the verification process resulted in an error (for instance, failed to open SSH connection with the network device, or the network device is unavailable), or if there is any discrepancy between the policies

that are configured on Cisco ISE and the network device, an alarm with a Warning icon is displayed for each of these network devices.

The **Verify Deployment** option is also available on the following pages:

- **Work Centers > TrustSec > Components > Security Groups**
- **Work Centers > TrustSec > Components > Security Group ACLs**
- **Work Centers > TrustSec > TrustSec Policy > Egress Policy > Matrix**
- **Work Centers > TrustSec > TrustSec Policy > Egress Policy > Source Tree**
- **Work Centers > TrustSec > TrustSec Policy > Egress Policy > Destination Tree**

Check the **Automatic Verification After Every Deploy** check box if you want Cisco ISE to verify the updates on all the network devices after every deployment. When the deployment process is complete, the verification process is started after the time that you specify in the **Time after Deploy Process** field. The current verification process is cancelled if a new deployment request is received during the waiting period or when the verification is in progress. Click **Verify Now** to start the verification process immediately.

IPv6 addresses can be used in IP SGT static mappings. These mappings can be propagated using SSH or SXP to specific network devices or network device groups.

If FQDN and hostnames are used, Cisco ISE looks for the corresponding IP addresses in the PAN and PSN nodes while deploying the mappings and checking the deployment status. You can select one of the following options (under **IP SGT Static Mapping of Hostnames**) in the **General TrustSec Settings** window to specify the number of mappings created for the IP addresses returned by the DNS query:

- **Create mappings for all IP addresses returned by DNS query**
- **Create mappings only for the first IPv4 address and the first IPv6 address that is returned by a DNS query**

Business Outcome

- Verifies TrustSec policy on Network Devices.
- Enhanced IP-SGT mapping workflow:
 - Improves network device misconfiguration error handling and operational efficiency through Check Status option.
 - Selectively deploy the IP SGT static mappings.
 - Create IP static mappings with IPv6 addresses.
 - Create mappings for first or all known IP addresses which are based on DNS FQDN query.

Decommissioned Dashlets

Some Dashlets Removed to Resolve Performance Issues

The following dashlets have been decommissioned to prevent performance issues when displaying large data sets:

- [Context Visibility > Endpoint > Compliance: Status Trend](#)
- [Home > Endpoints > Endpoint](#)

A large number of endpoints caused performance problems with some dashlets.

Known Limitations

Profiler RADIUS Probe

When the RADIUS probe is disabled, endpoints are not profiled but are only authenticated and added to the database.

High Memory Utilization

Cisco ISE Version 1.3 and later use RHEL, version 6. You may experience high memory utilization after installing or upgrading to Cisco ISE Version 1.3 or later. However, this does not negatively impact Cisco ISE performance and there are no alarms that are triggered. In case, if the memory usage is consistently above 90% or if there is any performance impact, you can contact Cisco TAC for troubleshooting.

Diffie-Hellman Minimum Key Length

Connection to LDAP server will fail if the Diffie-Hellman minimum key length configured on the LDAP server is less than 1024.

ECDSA Certificates

Elliptic Curve Digital Signature Algorithm (ECDSA) certificates that are used for EAP authentication are supported only for the endpoints with Android Version 6.x and later.

Cisco ISE supports ECDSA certificates with key lengths of 256 and 384 only. You can select the key length in the **Administration > System > Certificates > Certificate Management > System Certificates** window.



Note

Apple iOS is not supported if you use ECDSA as a system certificate. ECDSA certificates are supported only for Android 6.x and Android 7.x.

Cisco Temporal Agent

We recommend that you run the Cisco Temporal Agent within two minutes of downloading the agent from the Client Provisioning Portal. Otherwise, the `Posture Failed Due to Server Issues` error message is displayed.

Upgrade Information

- [Upgrading to Release 2.4 Patch 1](#)
- [Upgrading to Release 2.4](#)
- [Upgrade Packages](#)

- [License Information](#)
- [Upgrade Procedure](#)

Upgrading to Release 2.4 Patch 1

This section provides information on patches that were made available after the initial availability of the Cisco ISE 2.4 release. Patches are cumulative such that any patch version also includes all fixes delivered in the preceding patch versions. Cisco ISE version 2.4.0.357 was the initial version of the Cisco ISE 2.4 release. After installation of the patch, you can see the version information from **Settings > About Identity Services Engine** page in the Cisco ISE GUI and from the CLI in the following format “2.4.0.357 patch N”; where N is the patch number.



Note Within the bug database, issues resolved in a patch have a version number with different nomenclature in the format, “2.4(0.9NN)” where NN is also the patch number, displayed as two digits. For example, version “2.4.0.298 patch 1” corresponds to the following version in the bug database “2.4(0.901)”.



Note We recommend you to clear your browser cache after you install a patch on Cisco ISE, Release 2.4.

Upgrading to Release 2.4

You can directly upgrade to Release 2.4 from the following Cisco ISE releases:

- 2.0
- 2.0.1
- 2.1
- 2.2
- 2.3

If you are on a version earlier than Cisco ISE, Release 2.0, you must first upgrade to one of the releases listed above and then upgrade to Release 2.4.

You can upgrade to Release 2.4 from the GUI or the CLI.

Supported Operating System for Virtual Machines

Release 2.4 supports Red Hat Enterprise Linux (RHEL) 7.0.

If you are upgrading Cisco ISE nodes on a VMware VM, after you upgrade, ensure that you change the guest operating system to Red Hat Enterprise Linux (RHEL) 7. To do this, you must power down the VM, change the guest operating system to RHEL 7, and power on the VM after the change.

Upgrade Packages

Available upgrade packages, and the platforms they support, can be found on the [Cisco ISE Software Download](#) web site.

License Information

For licensing information, refer to the **Cisco ISE Licenses** chapter in the Cisco Identity Services Administrator Guide, Release 2.2.1.

Device Administration Licenses

For Cisco ISE 2.3 and earlier versions, a perpetual Device Administration license is required per deployment, regardless of the number of device administration nodes in the deployment. Starting from Cisco ISE 2.4, the number of Device Administration licenses must be equal to the number of device administration nodes (PSNs configured for device administration service) in a deployment.

If you are currently using a Device Administration license and plan to upgrade to Release 2.4, TACACS+ features will be supported for 50 Device Administration nodes in Release 2.4.

If you install a PAK generated from a new PID, Device Administration license count is displayed as per the quantity available in the PAK file. You can add multiple Device Administration licenses to your deployment based on the number of Device Administration nodes that you require. Evaluation license supports one Device Administration node.

Licenses for VM nodes

Cisco ISE is also sold as a virtual appliance. For Release 2.4, it is recommended that you install appropriate VM licenses for the VM nodes in your deployment. You must install the VM licenses based on the number of VM nodes and each VM node's resources such as CPU and memory. Otherwise, you will receive warnings and notifications to procure and install the VM license keys in Release 2.4, however, the services are not interrupted.

VM licenses are offered under three categories—Small, Medium, and Large. For instance, if you are using 3595 equivalent VM node with 8 cores and 64 GB RAM, you might need a Medium category VM license, if you want to replicate the same capabilities on the VM. You can install multiple VM licenses based on the number of VMs and their resources as per your deployment requirements.

VM licenses are Infrastructure licenses, therefore, you can install VM licenses irrespective of the endpoint licenses available in your deployment. You can install a VM license even if you have not installed any Evaluation, Base, Plus, or Apex license in your deployment. However, in order to use the features enabled by the Base, Plus, or Apex licenses, you must install the appropriate licenses.

After installing or upgrading to Release 2.4, if there is any mismatch between the number of deployed VM nodes and installed VM licenses, alarms are displayed in the Alarms dashlet for every 14 days. Alarms are also displayed if there are any changes in the VM node's resources or whenever a VM node is registered or deregistered.

VM licenses are perpetual licenses. VM licensing changes are displayed every time you log in to the Cisco ISE GUI, until you check the "Do not show this message again" check box in the notification popup.

If you have not purchased any ISE VM license before, refer to the [ISE Ordering Guide](#) to choose the appropriate VM license to be purchased. If you have purchased ISE VM licenses with no Product Authorization Key (PAK) associated, you can request VM PAKs by reaching out to ise-vm-license@cisco.com with Sales Order numbers that reflect the ISE VM purchase. This request will be processed to provide one medium VM license key for each ISE VM purchase you made in the past.

The following table shows how the VM resources are categorized:

VM Category	RAM Range	Number of CPU Cores
Small	16 GB	up to 6 cores

VM Category	RAM Range	Number of CPU Cores
Medium	greater than 16 GB to 64 GB	7 or 8 cores
Large	greater than 64 GB	greater than 8 cores

For more information about the licenses, see the "Cisco ISE Licenses" chapter in the *Cisco Identity Services Engine Administrator Guide, Release 2.4*.

Upgrade Procedure

Pre-requisites

- The Upgrade Readiness Tool (URT) should be run prior to an ISE software upgrade in order to detect and fix any data upgrade issues. Most upgrade failures occur because of data upgrade issues and the URT is designed to validate the data before the actual upgrade. The URT will report and try to fix the issues, wherever possible. The URT is a separate download in the Cisco ISE Download Software Center.
- Cisco recommends that you install all relevant patches before beginning the upgrade.

Do not begin the upgrade until you have read the Cisco Identity Services Engine Upgrade Guide, Release 2.2.

Cisco ISE Live Updates

Cisco ISE Live Update portals help you to automatically download Supplicant Provisioning Wizard, Cisco NAC Agent for Windows and Mac OS X, AV/AS support (Compliance Module), and agent installer packages that support client provisioning and posture policy services. These live update portals should be configured in Cisco ISE upon initial deployment to retrieve the latest client provisioning and posture software directly from Cisco.com to the Cisco ISE appliance.

If the default Update Feed URL is not reachable and your network requires a proxy server, you must configure the proxy settings in **Administration > System > Settings > Proxy** before you access the Live Update portals. If proxy settings are enabled to allow access to the profiler, posture and client provisioning feeds, it will break access to the MDM server as Cisco ISE cannot bypass proxy services for MDM communication. To resolve this, you can configure the proxy service to allow communication to the MDM servers. For more information on proxy settings, see the "Specify Proxy Settings in Cisco ISE" section in the "Administer Cisco ISE" chapter of the *Cisco Identity Services Engine Administrator Guide, Release 2.4*.

Client Provisioning and Posture Live Update Portals

You can download Client Provisioning resources from <https://www.cisco.com/web/secure/spa/provisioning-update.xml>

The following software elements are available at this URL:

- Supplicant Provisioning wizards for Windows and Mac OS X Native Supplicants
- Windows versions of the latest Cisco ISE persistent and temporal agents
- Mac OS X versions of the latest Cisco ISE persistent agents
- ActiveX and Java Applet installer helpers
- AV/AS compliance module files

For more information on automatically downloading the software packages that become available at Client Provisioning Update portal to Cisco ISE, see the "Download Client Provisioning Resources Automatically" section in the "Configure Client Provisioning" chapter in the [Cisco Identity Services Engine Administrator Guide, Release 2.4](#).

You can download Posture updates from <https://www.cisco.com/web/secure/spa/posture-update.xml>

The following software elements are available at this URL:

- Cisco predefined checks and rules
- Windows and Mac OS X AV/AS support charts
- Cisco ISE operating system support

For more information on automatically downloading the software packages that become available at this portal to Cisco ISE, see the "Download Posture Updates Automatically" section in the "Configure Client Posture Policies" chapter in the [Cisco Identity Services Engine Administrator Guide, Release 2.4](#).

If you do not want to enable the automatic download capabilities, you can choose to download updates offline.

Cisco ISE Offline Updates

This option allows you to download client provisioning and posture updates when direct Internet access to Cisco.com from a Cisco ISE appliance is not available or is not permitted by a security policy.

Offline updates are also available for Profiler Feed Service. For more information, see the [Configure Profiler Feed Services Offline](#) section in the *Cisco Identity Services Engine Administrator Guide*.

To download offline client provisioning resources:

Procedure

-
- Step 1** Go to the Download Software web page at: <http://www.cisco.com/cisco/software/navigator.html?a=a&i=rpm>.
- Step 2** Provide your login credentials.
- Step 3** Choose **Products > Security > Network Visibility and Enforcement > Cisco Identity Services Engine > Cisco Identity Services Engine Software**.

The following Offline Installation Packages are available for download:

- **win_spw-*<version>*-isebundle.zip**—Offline SPW Installation Package for Windows
- **mac_spw-*<version>*.zip**—Offline SPW Installation Package for Mac OS X
- **compliancemodule-*<version>*-isebundle.zip**—Offline Compliance Module Installation Package
- **macagent-*<version>*-isebundle.zip**—Offline Mac Agent Installation Package
- **nacagent-*<version>*-isebundle.zip**—Offline NAC Agent Installation Package
- **webagent-*<version>*-isebundle.zip**—Offline Web Agent Installation Package

- Step 4** Click either **Download** or **Add to Cart** .
-

For more information on adding the downloaded installation packages to Cisco ISE, see the "Add Client Provisioning Resources from a Local Machine" section in the "Configure Client Provisioning" chapter in the [Cisco Identity Services Engine Administrator Guide, Release 2.4](#).

You can update the checks, operating system information, and antivirus and antispyware support charts for Windows and Macintosh operating systems offline from an archive on your local system using posture updates.

For offline updates, you need to ensure that the versions of the archive files match the version in the configuration file. Use offline posture updates when you have configured Cisco ISE and want to enable dynamic updates for the posture policy service.

To download offline posture updates:

Procedure

- Step 1** Go to <https://www.cisco.com/web/secure/spa/posture-offline.html>.
Save the **posture-offline.zip** file to your local system. This file is used to update the operating system information, checks, rules, and antivirus and antispyware support charts for Windows and Macintosh operating systems.
- Step 2** Launch the Cisco ISE administrator user interface and choose **Administration > System > Settings > Posture**.
- Step 3** Click the arrow to view the settings for posture.
- Step 4** Click **Updates**.
The **Posture Updates** window is displayed.
- Step 5** Click the **Offline** option.
- Step 6** Click **Browse** to locate the archive file (posture-offline.zip) from the local folder on your system.
- Note** The **File to Update** field is a required field. You can select only a single archive file (.zip) that contains the appropriate files. Archive files other than .zip, such as .tar, and .gz are not allowed.
- Step 7** Click **Update Now**.
-

Configuration Information

Pre-requisites

- Provided the relevant Cisco ISE license fee(s).
- The latest patches are installed.
- Verified that the Cisco ISE software capability is active.
- Reviewed the related Release Notes for this release of Cisco Identity Services Engine.

Refer to the following to get started with configuring ISE:

- [Getting started with ISE](#)
- Videos on the [Cisco ISE Channel on YouTube](#)
- [ISE Design and Integration Guides](#)
- *Cisco Identity Services Engine Administrator Guide*

Monitoring and Troubleshooting Information

For information on monitoring and troubleshooting the system, refer to the Monitoring and Troubleshooting Cisco ISE section in the *Cisco Identity Services Administrator Guide*.

Ordering Information

For detailed Cisco ISE ordering and solution sales information, consult the following:

- [Cisco Identity Services Engine Ordering Guide](#)
- [Cisco Sales Connect](#)
- [ISE Instant Demo](#)
- [ISE Sales Training](#)
- [Other ISE Demos & PoVs](#) (includes YouTube and dCloud demos, dCloud PoVs, and Onsite/Lab PoVs)
- [Selling ISE](#)
 - [Selling ISE EN Generalist](#)
 - [Selling ISE for Security](#)
- [Selling ISE Questions?](#)

Cisco ISE Integration with Other Cisco Products

SDA and DNA

You can manage and automate your network - including policy and access - from a single dashboard with [Cisco DNA Center](#). DNA Center is a holistic, end-to-end network management platform for the [Network Intuitive](#). Integrating ISE allows the DNA Center to define and enact policy to control access across the network, all from a unified interface. Cisco ISE 2.3 is a required integration component for the DNA Center, along with [APIC-EM](#) and the [Network Data Platform](#), which all make up the [Software-Defined Access](#) solution.

Also refer to the [What's New in ISE 2.4?](#) web site and to the [ISE Policy User Interface Walkthrough](#) YouTube video.

Migration Information

For information on migrating from ACS to ISE, see the [Cisco Identity Services Engine, Release 2.4 Migration Tool Guide](#).

Caveats

This section describes open severity 1 and 2 caveats and select severity 3 caveats. The “Open Caveats” sections list open caveats that apply to the current release and may apply to previous releases. A caveat that is open for a prior release and is still unresolved applies to all future releases until it is resolved. The bug IDs are sorted alphanumerically. The Caveats section includes the bug ID and a short description of the bug. For details on the symptoms, conditions, and workaround for a specific caveat, you must use the Bug Search Tool.

Cisco Bug Search Tool (BST), the online successor to Bug Toolkit, is designed to improve effectiveness in network risk management and device troubleshooting. You can search for bugs based on product, release, and keyword, and aggregates key data such as bug details, product, and version. For more details on the tool, see the help page located at <http://www.cisco.com/web/applicat/cbsshelp/help.html>.

Cisco ISE, Release 2.4.0.357, Patch 1, Resolved Caveats

Table 2: Cisco ISE, Release 2.4.0.357, Patch 1, Resolved Caveats lists the issues that are resolved in Cisco Identity Services Engine, Release 2.4 cumulative patch 1. To obtain the patch file necessary to apply the patch to Cisco ISE, Release 2.4, log in to the Cisco Download Software site at <http://www.cisco.com/cisco/software/navigator.html?a=a&i=rpm> (you might be required to provide your Cisco.com login credentials), navigate to **Security > Access Control and Policy > Cisco Identity Services Engine > Cisco Identity Services Engine Software**, and save a copy of the patch file to your local machine.

Patch 1 might not work with older versions of SPW. MAC users need to upgrade their SPW to MACOSXSPWizard 2.2.1.43 or later and Windows users need to upgrade their SPW to WinSPWizard 2.1.0.53 or later

Then refer to the “[Installing a Software Patch](#)” section of the “Administer Cisco ISE” chapter of the Cisco Identity Services Engine Administrator Guide, Release 2.4. for instructions on how to apply the patch to your system.

Table 2: Cisco ISE, Release 2.4.0.357, Patch 1, Resolved Caveats

Caveat	Description
CSCvi36111	Live sessions - NAS IP address Tooltip is duplicated for ipv6
CSCvi47074	Replication failure seen on SXP nodes during SXP connection down
CSCvi48886	Post upgrade - the GuestVLAN doesn't copy the key of omapi.key to DHCP
CSCvi50979	Machine change password interval should be configurable from advance tuning parameter (Kerberos SSO)
CSCvi56003	AUP Link in the Self-Registration form throws Bad Request in ISE 2.4
CSCvi69286	Dashboard > Search : Endpoint details screen doesn't work correctly in Internet Explorer

Caveat	Description
CSCvj11476	ISE : Wrong error message when deleting a certificate referenced by some resource
CSCvi53593	Wrong msg if trying to issue CoA and no MAC address is selected
CSCvj61368	2.4 P1: ISE Indexing server is not running on secondary PAN
CSCvi38373	ISE Delete All Endpoints in Context Visibility too risky
CSCvh93370	ISE Guest: Incorrect accounting in syslog causes issues
CSCvi06647	Anyconnect configuration - drop menu for compliance module is empty
CSCvi61330	Occasional application restart post Radius/DTLs authentication
CSCvg90863	"Application Configure ISE" left idle for long time causes SSHD to disable
CSCvj17258	ISE 2.4 keeps old DNAC client cert causing new DNAC pxGrid with ISE to fail
CSCvj33336	DNAC1.2: Network devices not getting added in ISE 2.4 after provision
CSCvi49103	Wrong data type for "Enable Multi Shared Secret:String(128)" in NAD CSV export
CSCvg19708	Guest Accounting report broken

Cisco ISE, Release 2.4, Open Caveats

The following table lists the open caveats in Release 2.4.

Table 3: Cisco ISE, Release 2.4, Open Caveats

Caveat	Description
CSCvi36111	NAS IP Address Tooltip is duplicated for ipv6.
CSCvi41578	Portal redirection is not supported in Chrome 65 for Win10.
CSCvi48276	AMP Adapter is connected even after deregistering/deauthorizing from AMP cloud.
CSCvi48298	Policy Hit count value gets nullified while creating new policies in a specific case.

CSCvi50979	Machine change password interval should be configurable from advance tuning parameter (Kerberos SSO).
CSCvh07648	Restore/Upgrade fails when authorization policy has an MDM server condition but the respective server is disabled.
CSCvi69286	Dashboard > Search : Endpoint details screen does not work in Internet Explorer.

Cisco ISE, Release 2.4, Resolved Caveats



Note Cisco ISE 2.4 has parity with Cisco ISE 2.0 Patch 6, 2.0.1 Patch 5, 2.1 Patch 6, 2.2 Patch 6, and 2.3 Patch 2

The following table lists the resolved caveats in Release 2.4.

Table 4: Cisco ISE, Release 2.4, Resolved Caveats

Caveat	Description
CSCvf69805	Cisco Identity Services Engine cross-site request forgery vulnerability
CSCvf49844	Cisco Identity Services Engine local command injection vulnerability Note The context visibility sync option and reset commands can be found in Release 2.4.
CSCvf63414	Cisco Identity Services Engine authenticated CLI denial of service vulnerability
CSCvh51992	Cisco Identity Services Engine authenticated CLI denial of service vulnerability
CSCvf69753	Cisco Identity Services Engine authenticated privilege escalation vulnerability
CSCvf69963	Cisco Identity Services Engine cross-site scripting vulnerability
CSCvg95479	Cisco Identity Services Engine command injection to underlying OS vulnerability
CSCvd38467	BYOD does not work on Apple iOS 10.3.x.
CSCvf29467	Editing multiple client provisioning policies simultaneously hides the results column.
CSCvf33475	Simultaneous configuration and operational backup on same browser is very slow.

CSCvi45925	Newly created dashboard not visible in 2.4 342 build.
CSCvf28877	ISE 2.3 TACACS+ : Unable to add commands to Command Set while editing.
CSCvf32298	ISE 2.3 Sponsor Portal: There is a delay of one minute between the update of the username table and the counter.
CSCvf32394	ISE 2.3 Self-registered guest portal of SMS provider- Global default is always re-selected when other attributes are changed.
CSCvf34216	ISE 2.3: Unable to select Work Center Menu - Guest Access Identity Group upon opening detailed report.
CSCvh05703	'Remember Me' RADIUS live sessions view does not show usernames for guest devices

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see [What's New in Cisco Product Documentation](#).

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the . RSS feeds are a free service.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2018 Cisco Systems, Inc. All rights reserved.